COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

CONGRESSMAN ADAM PUTNAM, CHAIRMAN

STATEMENT OF THE CHAIRMAN
FEDERAL COMPUTER SECURITY REPORT CARD
December 9, 2003

For too long now information security has taken a back seat in the collective conscience of our nation. We must come to the stark realization that a major Achilles heel is our computer networks. Unfortunately, the history of our nation -- in heeding warnings of imminent danger -- doesn't lend itself to very much optimism.

The tragic events of 9/11 were foreshadowed by a number of signs that were ignored or not taken seriously. Al-Queda was long known to be conspiring to hijack planes and crash them into key buildings both here and across the Atlantic. Back as far as 1994 plots were uncovered to crash planes into the Eiffel Tower, CIA Headquarters and blow up U.S. planes while crossing the Atlantic. We failed to adequately heed these warnings, and we all know the eventual tragic result.

The writing is once again on the wall. The choice before us is a clear one: Inaction resulting in eventual economic devastation and potentially catastrophic loss of life, or preemptive action to protect our Nation. I, for one, vote for ACTION and today as I stand before you I recommit the resources of my Subcommittee to doing everything we can to ensure we adequately protect our nation against cyber attack.

While the choice is clear, the terrain is difficult and the enemy cunning. Sometimes in fact, the worst enemy is the enemy within. The culture of our top level CEO's in the private sector, and top executives in government must be changed. We must get those at the very top, the decision makers, the ones accountable to the shareholders, the customers or the electorate, to recognize that lack of network security in an organization is a material weakness and one that deserves necessary resources and immediate action.

As many of you know, a few weeks ago I circulated draft legislation that would work through the SEC to require publicly traded companies to report on their computer

security. The draft legislation definitely got many people's attention. Numerous companies and associations approached me and asked if we, Congress, would provide the private sector a chance to do this on their own without government regulation.

That approach is actually my preference. Therefore, I formed the Corporate Information Security Working Group. The goal is to come up with set of information security best practices and guiding principles that would be adopted – voluntarily – by the private sector. This group has met twice and I'm hopeful that we can reach a successful conclusion by later winter or early spring.

It should also be noted that as part of the National Cyber Security Summit held last week in Santa Clara, California there was a Corporate Governance Task Force, as one of five working groups, and their works dovetails nicely with the work of the Corporate Information Security Working Group.

The Internet has been an amazing business tool and has helped this economy grow to once unimaginable heights. President Bush's National Security Advisor, Condoleezza Rice has said, "Today, the cyber-economy is the economy…Corrupt those networks and you disrupt this nation." I couldn't agree more. The complexity of the securing our networks should not be underestimated either.

The ability for us to have open yet secure networks will be the key to this Nation thriving in the digital economy. However, as I approach the end of my first year as Subcommittee Chairman, I have come to realize that there are many impediments to a successful conclusion.

I see our digital security divided up into several key areas: Home computers, private enterprise, academia and lastly -- the federal, state and local governments. Although not directly part of our critical infrastructure, home computers represent a serious weakness in our national security. With the advent of broadband, always-on connections are open invitations for trouble.

While some burden is on the shoulders of the user, I feel strongly that a significant burden falls on the shoulders of the hardware, software, operating system manufacturers, and ISPs. These entities, until recently have paid insufficient attention to educating consumers as to the importance of security.

While billions of dollars have been spent to advertise the benefits of products such as speed and ease of use, the security component has been neglected.

The average home user just doesn't know how vulnerable their home computer is, and how important it is to have firewalls, virus protection and to install the updates or security patches as soon as they become available. We must do more and when I say "we", I am including the Federal government. We must make it a priority to educate home users.

And, since I just mentioned it, let me take a minute to talk about patch management. It's simply too difficult. Patches that are confusing, time consuming to apply, or too difficult to uninstall in the event of a problem, are patches that are less likely to be downloaded by the home user. It's imperative that manufactures make patches easier to understand and install. Some companies are moving towards automatic updates that do not require user action.

While once companies shied away from this notion in order to protect the sovereignty of the home user's computer, it is becoming evident that something else needs to be done. Automatic updates, in all likelihood, may require some congressional action in order to be successfully deployed and the Subcommittee is actively exploring this area.

Additionally, more products must be delivered to consumers – secure -- out-of-the-box. Security defaults should set to ON, and the consumer should have to turn them off if they so desire. This summer I visited almost a dozen prominent companies in Silicon Valley.

I came away with several important perspectives. The industry is paying attention to what's going on in the real world. Industry is trying to improve. And, I need to get out of DC more often. I say this in all seriousness because, unfortunately, this is not a town of the "can do." It's often the town of the "it can't be done, and let me tell you all the reasons why." It was refreshing to be in a "can do" environment where you're limited in many ways only by your imagination.

However, no discussion of Silicon Valley and the industry, in general, would be complete without talking about the quality of software being developed today. Simply, we can and must do better.

While software is certainly complicated, with millions of lines of code, there are just some basics that clearly aren't being addressed. There is compelling evidence that would suggest that security has not been routinely built into the product during development, rather it is addressed following deployment…seemingly not the most efficient or productive approach in today's threatening climate.

NIST estimates that software bugs and errors costs the U.S. economy $59.5 billion per year. We can and must do better. If the industry doesn't act, Congress will be forced to. I can't overemphasis the importance of securing the Nation's computers and networks.

The threat of cyber attack is real. The damage that could be inflicted both in terms financial loss and, potentially loss of life, is considerable. It is estimated that the recent SoBig-F virus caused more than $10 billion in economic losses. And it didn't even have a malicious payload! If the payload had changed or erased data, who knows what the cost could have been. Although most of our critical infrastructure assets are in private control, the Federal Government should be the leader when it comes to information security.

Worms and viruses continue to get more malicious by the day. The time between vulnerability and exploit is closing rapidly. For *Slammer*, the time from discovery to exploit was six months, and this summer *Blaster* was created in three weeks. Zero day exploits cannot be far away.

Not only must we work harder on the software side of the equation, the Federal government must do a better job of tracking, capturing and successfully prosecuting those that inflict digital destruction on our Nation's computer network. The Subcommittee is currently engaged with the Justice Department and FBI to explore the current tools available to law enforcement both domestically and internationally in this arena, and what more might need to be done.

Today the Subcommittee is releasing the 2003 Federal Computer Security Score Card. This is the 4th year the scores will be released following the process started by former Congressman Stephen Horn.

This year, for the first time, the grades will be based on the Federal Information Security Management Act (FISMA) that was passed by Congress last year.

Chairman Tom Davis has been a leader in information security and through his FISMA legislation, he has laid the groundwork for better security and better reporting for the government's computer systems. This year's grades were based on the FISMA reports that the agencies provided to Congress and the Office of Management and Budget in September.

OMB has worked hard to advance computer security at all the Federal agencies and we have consulted OMB on the scorecard. I would also like to thank the GAO for their help in preparation of these grades. This year is an important grading year because for the first time we can accurately compare the agencies to a previous year because the grading requirements changed very little.

- This year overall the Federal Government gets a grade of D. That's an improvement over the F the government received last year.

- For the first time, two agencies (The Nuclear Regulatory Commission and the National Science Foundation) have received As.

- 14 agencies have increased their grades this year.

- Only five agencies have completed reliable inventories of their critical IT assets leaving 19 without reliable inventories. This is very troubling considering we are four years into this process and still we have far too many agencies with incomplete inventories. How can you secure what you don't know you have?

- The IGs of three agencies (DoD, Veterans Affairs, and Treasury) did not submit independent reports. I must stress the IG component of this equation is critically important.

The independent verification is vital and particularly in light of the fact that there were significant differences between many of the agencies and their IGs. 7 agencies had difference of two grades or more with their IGs.

- 14 agencies are still below a C and eight have failed

As we worked on these grades, there were some overriding themes that became apparent for the agencies with good grades vs. those with poor grades.

Those producing more favorable results:
- A full inventory of their critical IT assets.
- Identified critical infrastructure and mission critical systems.
- A strong incident identification and reporting procedures.
- Tight controls over contractors.
- Strong plans of actions and milestones that serve as guides for finding and eliminating security weaknesses

The Nuclear Regulatory Commission and the National Science Foundation should be commended for their outstanding scores, as well as the Social Security Administration and the Department of Labor for their B+ and B respectively, as well as the agencies that moved from an F to a C. And, while DHS had a failing grade we recognize the difficult reorganization that took place and we expect significant improvement next year.

While the overall grade of the federal government did improve, progress is still too slow for my satisfaction. We must do more and do it quicker if we are going to protect ourselves from a potential digital disaster. In the coming weeks, the Subcommittee will be in direct contact with the agency CIOs and we will work with them on plans of action and milestones to improve their grades. OMB has a report of its own, which will be released on March 1, and I would expect to hold a hearing shortly after that. Additionally, I will be in contact with the Appropriations Committee to make them aware of the grades for the agencies and also to stress the importance of adequate funding for information security.

Thank you for coming and I will answer any questions you may have. If you have specific agency questions, the Subcommittee staff will remain here to assist you.